MULTIMEDIA UNIVERSITY

STUDENT ID NO

MULTIMEDIA UNIVERSITY

FINAL EXAMINATION

TRIMESTER 3, 2017/2018

TAC3121 – APPLIED CRYPTOGRAPHY

(All sections / Groups)

6 JUNE 2018
2.30 p.m. - 4.30 p.m.
(2 Hours)

INSTRUCTIONS TO STUDENTS

1. This question paper consists of 3 pages including the cover page with **FIVE** questions only.

2. Attempt **ALL** questions. All questions carry equal marks and the distribution of the marks for each question is given.

3. Please print all your answers in the Answer Booklet provided.

Question 1

(a) What is Kerchoffs' Principle? [2 marks]

(b) Why in general public key cryptosystems are slower than private key cryptosystems? [2 marks]

(c) List the THREE (3) adversarial goals for a public key encryption scheme. [3 marks]

(d) List THREE (3) possible approaches to attack RSA. [3 marks]

Question 2

(a) Solve for GCD(990, 378). Show the steps. [2 marks]

(b) Using the 2-row Rail Fence cipher, decrypt the following ciphertext:

TEESOUSIUEOHRWRHRINSBTTTFRADOK [4 marks]

(c) Decrypt the following ciphertext using Vigenere Cipher with the keyword *great*:

YFERBTX YPPGIHS [4 marks]

Question 3

(a) Show how Key Generation, Encryption and Decryption are performed given the following El Gamal parameters: prime, $p = 11$; generator, $g = 2$; private key, $x = 3$; plaintext, $m = 9$ (assuming the randomly chosen $k = 6$). [5 marks]

(b) Users A and B use the Diffie-Hellman key exchange technique with a common prime $q = 71$ and a primitive root $\alpha = 7$.

i. Calculate A's public key Y_A if user A has private key $X_A = 5$. [2 marks]
ii. Calculate B's public key Y_B if user B has private key $X_B = 12$. [2 marks]
iii. Calculate the shared secret key? [1 mark]

Continued...

Question 4

(a) Describe and give an usage example for Electronic Codebook (ECB). [3 marks]

(b) The middle portion of triple DES is a decryption rather than an encryption. Comment on the statement given. [3 marks]

(c) State FOUR (4) different ways to distribute public keys. [4 marks]

Question 5

(a) Explain how a hash function is used to create digital signatures with the help of a diagram. [4 marks]

(b) Explain how digital signature is used in public key certification. [3 marks]

(c) What is the difference between a message authentication code and a one-way hash function? [3 marks]

End of Page